H.R. 3523 – Cyber Intelligence Sharing and Protection Act of 2011 (CISPA)

Key Concerns
Congresswoman Zoe Lofgren (D-CA)

- **CISPA could allow any private company to share vast amounts of sensitive, private data about its customers with the government.** CISPA would override all other federal and state privacy laws, and allow a private company to share nearly anything—from the contents of private emails and Internet browsing history to medical, educational and financial records—as long as it "directly pertains to" a "cyber threat," which is broadly defined.

- **CISPA does not require that data shared with the government be stripped of unnecessary personally-identifiable information.** A private company may choose to anonymize the data it shares with the government. However, there is no requirement that it does so—even when personally-identifiable information is unnecessary for cybersecurity measures. For example, emails could be shared with the full names of their authors and recipients. A company could decide to leave the names of its customers in the data it shares with the government merely because it does not want to incur the expense of deleting them. This is contrary to the recommendations of the House Republican Cybersecurity Task Force and other bills to authorize information sharing, which require companies to make a reasonable effort to minimize the sharing of personally-identifiable information.

- **CISPA would allow the government to use collected private information for reasons other than cybersecurity.** The government could use any information it receives for "any lawful purpose" besides "regulatory purposes," so long as the same use can also be justified by cybersecurity or the protection of national security. This would provide no meaningful limit—a government official could easily create a connection to "national security" to justify nearly any type of investigation.

- **CISPA would give Internet Service Providers free rein to monitor the private communications and activities of users on their networks.** ISPs would have wide latitude to do anything that can be construed as part of a "cybersecurity system," regardless of any other privacy or telecommunications law.

- **CISPA would empower the military and the National Security Agency (NSA) to collect information about domestic Internet users.** Other information sharing bills would direct private information from domestic sources to civilian agencies, such as the Department of Homeland Security. CISPA contains no such limitation. Instead, the Department of Defense and the NSA could solicit and receive information directly from American companies, about users and systems inside the United States.

- **CISPA places too much faith in private companies, to safeguard their most sensitive customer data from government intrusion.** While information sharing would be voluntary under CISPA, the government has a variety of ways to pressure private companies to share large volumes of customer information. With complete legal immunity, private companies have few clear incentives to resist such pressure. There is also no requirement that companies ever tell their customers what they have shared with the government, either before or after the fact. As informed consumers, Americans expect technology companies to have clear privacy policies, telling us exactly how and when the company will use and share our personal data, so that we can make informed choices about which companies have earned our trust and deserve our business.